■ อรุพจน์ กัลยาสิริ

ตรวจจับผู้บุกรุก : รูปแบบการโจมตี

จำแนกกลุ่มของการบุกรุกอย่างชัดเจนและมีเหตุผลทั้งในอดีตและปัจจุบัน

ระบบคอมพิวเตอร์ที่ถูกทำลายจากผู้ไม่ประสงค์ดีจะเกิดความเสียหายมากหรือน้อยขึ้นอยู่กับรูปแบบของการบุกรุก เนื่องจากวิธีการเข้ามาทำลายระบบคอมพิวเตอร์มีหลากหลายรูปแบบโดยทั้งในอดีตและปัจจุบันมีการบุกรุกเกิดขึ้นมากมาย แต่ละชนิดก็มีความแตกต่างกันทั้งในแง่ของพฤติกรรมและผลที่เกิดขึ้นจากการบุกรุกนั้น วิธีการบุกรุกต่าง ๆ เหล่านี้มีมากมายจนในบางครั้งอาจทำให้สับสนและไม่สามารถอธิบายได้อย่างถูกต้องและมีหลักการเพียงพอ ในช่วงเวลาสิบปีที่ผ่านมามีงานวิจัยที่เกี่ยวข้องกับระบบรักษาความปลอดภัยของคอมพิวเตอร์มากมายที่พยายามจะจัดกลุ่มและจำแนกวิธีการบุกรุกของผู้ไม่ประสงค์ดีเป็นกลุ่ม ๆ ให้ง่ายต่อการทำความเข้าใจ

ในปัจจุบันมีบทความและเอกสารจำนวนมากที่อธิบายถึงวิธีการบุกรุกของแฮกเกอร์หรือแครกเกอร์ ซึ่งโดยส่วนใหญ่ข้อมูลที่นำเสนอเหล่านั้นจะหยิบยกวิธีการที่มักเป็นที่นิยมใช้กันและสามารถสร้างความเสียหายให้แก่ระบบได้ง่าย พฤติกรรมการบุกรุกต่าง ๆ ดังกล่าวจะมีการทำงานที่ชัดเจนและเป็นที่รู้จักกันเป็นอย่างดีและแพร่หลาย นอกจากนั้นยังมีการอธิบายรูปแบบการบุกรุกจำนวนมากที่มักอ้างอิงจากแหล่งข้อมูลที่มีอยู่ในอินเทอร์เน็ตซึ่งในบางครั้งอาจจะซ้ำซ้อนและเกี่ยวพันกันจนไม่สามารถแบ่งแยกให้เข้าใจได้โดยง่ายและชัดเจนเพียงพอ ดังนั้นบุคคลที่มีความสนใจในวิทยาการด้านนี้จะค่อนข้างสับสนเนื่องจากเอกสารต่าง ๆ ก็มักจะเลือกรูปแบบการบุกรุกบางแบบขึ้นมาแล้วจัดกลุ่มโดยมิได้คำนึงถึงความเกี่ยวพันกันตามหลักการทางวิชาการมากนัก เพราะฉะนั้นหากจะศึกษาวิธีการบุกรุกให้แน่ชัดและถูกต้องแล้วจะต้องได้รับข้อมูลที่ครอบคลุมทั้งหมดภายใต้โครงสร้างที่ชัดเจน นอกจากนั้นสำหรับบุคคลที่มีหน้าที่รับผิดชอบต่อการรักษาความปลอดภัยให้แก่ระบบคอมพิวเตอร์แล้วก็ยิ่งจะต้องมีความรู้ความเข้าใจถึงพฤติกรรมการบุกรุกเป็นอย่างดีและพร้อมที่จะศึกษาข้อมูลเพิ่มเติมให้มีความรู้กว้างขวางขึ้นภายใต้ภูมิความรู้และหลักการที่ถูกต้อง

บทความตอนนี้จะอธิบายรูปแบบการบุกรุกระบบคอมพิวเตอร์อย่างมีหลักการโดยการจำแนกกลุ่มของการบุกรุกอย่างชัดเจนและมีเหตุผล เพื่อให้ผู้สนใจได้มองเห็นภาพรวมทั้งหมดของการบุกรุกที่เกิดขึ้นทั้งในอดีตและปัจจุบัน เพราะฉะนั้นในอนาคตหากได้ทราบพฤติกรรมการบุกรุกอื่นเพิ่มเติมขึ้นมาจากเดิมก็จะสามารถเข้าใจได้โดยง่ายและมีหลักการมากยิ่งขึ้น ซึ่งถือเป็นประโยชน์มากต่อการศึกษาข้อมูลเพิ่มเติมในวิทยาการแขนงนี้นั่นเอง

รูปแบบการบุกรุก

การบุกรุกระบบคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบันและในอดีตนั้นสามารถจำแนกได้เป็น 7 กลุ่ม ได้แก่

- การขโมยรหัสผ่าน (Stealing Password)
- พฤติกรรมทางสังคม (Social Engineering)
- ข้อผิดพลาดและจุดอ่อน (Bugs and Backdoors)
- ความผิดพลาดของการพิสูจน์ตัวจริง (Authentication Failures)
- ความผิดพลาดของโปรโตคอล (Protocol Failures)
- การรั่วไหลของข้อมูล (Information Leakage)
- การปฏิเสธการให้บริการ (Denial-of-Service)

การขโมยรหัสผ่าน

การขโมยรหัสผ่านถือเป็นวิธีการที่มักเกิดขึ้นโดยเป็นความพยายามที่จะเจาะเข้าสู่ระบบคอมพิวเตอร์ นั่นคือหากผู้บุกรุกสามารถทราบรหัสผ่านของผู้ใช้งานในระบบใด ๆ แล้วก็จะสามารถเข้าสู่ระบบนั้น ๆ ได้โดยเปรียบเสมือนเป็นบุคคลปกติ เพราะฉะนั้นหากสามารถหาวิธีการใด ๆ เพื่อให้ได้มาซึ่งรหัสผ่านแล้วก็จะสามารถสร้างความเสียหายอย่างอื่นกับระบบได้อีก แหล่งข้อมูลต่าง ๆ ในอินเทอร์เน็ตมีเครื่องมือหรือโปรแกรมมากมายที่ใช้สำหรับการเดารหัสผ่าน หลักการของโปรแกรมเหล่านี้คือการเปรียบเทียบและลองทดสอบสายอักขระที่คาดว่าจะเป็นรหัสผ่านกับคำในพจนานุกรมหรือการนำคำในพจนานุกรมมาต่อกัน เพราะฉะนั้นหากรหัสผ่านเป็นการตั้งขึ้นจากคำทั่วไปที่ทราบกันดีหรือเป็นคำศัพท์ในพจนานุกรมแล้ว โปรแกรมเดารหัสผ่านจะค้นหาและทราบได้โดยง่าย

ในระบบปฏิบัติการยูนิกซ์จะมีไฟล์สำหรับเก็บรหัสผ่านของบัญชีผู้ใช้งานในระบบไว้ ซึ่งตามปกติรหัสผ่านจะไม่สามารถอ่านได้โดยตรง นั่นคือจะเป็นอักขระที่ถูกเข้ารหัสไว้ แต่อักขระที่ถูกเข้ารหัสนั้นยังสามารถนำไปถอดรหัสได้หากมีโปรแกรมอัตโนมัติสำหรับการถอดรหัสที่มีประสิทธิภาพหรือจะสามารถทราบรหัสผ่านได้ง่ายขึ้นหากแฮกเกอร์ทราบกระบวนวิธีการเข้ารหัส

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
named:x:25:25:Named:/var/named:/bin/false
gdm:x:42:42::/home/gdm:/bin/bash
piranha:x:60:60::/home/httpd/html/piranha:/dev/null
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
pvm:x:24:24::/usr/share/pvm3:/bin/bash
squid:x:23:23::/var/spool/squid:/dev/null
```

รูปที่ 1 ตัวอย่างไฟล์เก็บรหัสผ่าน

ระบบปฏิบัติการรุ่นใหม่ในปัจจุบันจะไม่แสดงอักขระของรหัสผ่าน (ถึงแม้จะมีการเข้ารหัสแล้ว) ให้เห็นอย่างชัดเจน แต่จะเก็บไว้ในอีกแฟ้มซึ่งมักจะใช้ชื่อ **/etc/shadow** และมักจะไม่อนุญาตให้แก้ไขไฟล์นี้ได้โดยง่าย ด้วยวิธีการนี้จะช่วยลดปัญหาการเดารหัสผ่านลงไปได้พอสมควร รูปแบบของไฟล์เก็บบัญชีผู้ใช้งานและรหัสผ่านมักจะอยู่ใน **/etc/passwd** ดังรูปที่ 1

นอกจากการใช้โปรแกรมเดารหัสผ่านเพื่อให้ได้มาซึ่งรหัสผ่านแล้ว ยังมีวิธีการอื่น ๆ อีก เช่น การใช้ตัววิเคราะห์โปรโตคอลหรือสนิฟเฟอร์ วิเคราะห์และตรวจดูแพ็กเกตในเครือข่ายเพื่อมองหารหัสผ่านที่ปรากฏอยู่ แต่วิธีการนี้จะยุ่งยากหากแฮกเกอร์ไม่มีความรู้ด้านการสื่อสารของคอมพิวเตอร์เพียงพอ วิธีการป้องกันการลักลอบดูรหัสผ่านซึ่งปรากฏในแพ็กเกตทำได้โดยการเข้ารหัสข้อมูลก่อนการติดต่อสื่อสารผ่านเครือข่ายคอมพิวเตอร์ ทำให้แฮกเกอร์ไม่สามารถมองเห็นรหัสผ่านได้โดยตรง

พฤติกรรมทางสังคม

การบุกรุกที่จัดอยู่ในกลุ่มนี้จะค่อนข้างยากต่อการตรวจจับ เนื่องจากเป็นพฤติกรรมของคนซึ่งในบางครั้งยากต่อการคาดเดา พฤติกรรมทางสังคมที่เป็นสาเหตุของการบุกรุกระบบคอมพิวเตอร์ คือ ความพยายามใด ๆ ที่ทำให้เกิดการเข้าใจผิดหรือเกิดผลทำให้สามารถบุกรุกเข้ามาสร้างความเสียหายให้แก่ระบบได้ รูปแบบเหล่านี้มีมากมาย เช่น การไม่ทำหน้าที่รักษาความปลอดภัยอย่างรัดกุมเพียงพอ หรือการถูกหลอกจากผู้ไม่ประสงค์ดีจนเป็นผลให้เกิดการบุกรุกเกิดขึ้น ตัวอย่างเหตุการณ์นี้ได้แก่ ผู้ดูแลระบบได้รับจดหมายอิเล็กทรอนิกส์จากบุคคลที่รู้จักคนหนึ่งให้เปิดบัญชีอนุญาตเข้าสู่ระบบได้ ซึ่งจดหมายนี้เป็นจดหมายปลอมที่มากจากแฮกเกอร์นั่นเอง ตัวอย่างจดหมายแสดงในรูปที่ 2

```
From: research@host.domain.com
To: root@host.domain.com
Subject: Urgently request

Bill, we have a visitor professor coming next week. Could you add a login
account for him? Here's his password line; please use the same hashed
password.

profpxf:5bHD/k5k5mTTS:204:147:Prof.Pexo Flem:/home/pxf:/bin/sh

Thank you very much in advance.
Tom
```

รูปที่ 2 จดหมายปลอมของแฮกเกอร์

จดหมายอิเล็กทรอนิกส์ฉบับนี้เป็นการบอกให้ผู้ดูแลระบบ (Bill) เปิดบัญชีให้เข้าสู่ระบบได้ โดยบัญชีนี้ใช้ชื่อ profpxf ซึ่งแฮกเกอร์หลอกว่าเป็นศาสตราจารย์ที่มีความจำเป็นจะต้องใช้งานระบบคอมพิวเตอร์ หากผู้ดูแลระบบเชื่อในจดหมายนี้ก็จะอนุญาตให้แฮกเกอร์เข้าสู่ระบบได้โดยง่ายดาย

จะเห็นได้ชัดเจนว่าการบุกรุกที่อาศัยพฤติกรรมทางสังคมนี้สามารถป้องกันได้เช่นกัน ได้แก่ การไม่เชื่ออะไรง่าย ๆ โดยไม่พิจารณาให้ดีเสียก่อน การแก้ปัญหาในตัวอย่างข้างต้นสามารถทำได้โดยการติดต่อกลับไปที่ผู้ส่งจดหมายว่าได้ส่งจดหมายนั้นมาจริงหรือไม่ แต่หากให้แน่ชัดยิ่งขึ้นก็ควรจะติดต่อโดยตรงอาจผ่านทางโทรศัพท์หรือพบโดยตรงก็ได้

ข้อผิดพลาดและจุดอ่อน

ระบบคอมพิวเตอร์มักจะมีจุดอ่อนและข้อผิดพลาดเกิดขึ้นทั้งในโปรแกรมที่ใช้งานในระดับประยุกต์และแม้กระทั่งระบบปฏิบัติการหรือโอเอสเองก็อาจจะมีข้อบกพร่องเกิดขึ้นได้เช่นเดียวกัน จุดอ่อนและข้อผิดพลาดเหล่านี้อาจนำไปสู่การเจาะเข้าสู่ระบบคอมพิวเตอร์ได้ ดังนั้นหากผู้บุกรุกทราบข้อผิดพลาดและจุดอ่อนของระบบต่าง ๆ อย่างละเอียดแล้วจะทำให้สามารถทำลายระบบคอมพิวเตอร์เหล่านั้นได้ง่ายยิ่งขึ้น จุดอ่อนที่มักพบกันเสมอ ได้แก่ การทำงานที่ผิดพลาดของส่วนที่ให้บริการกับผู้ใช้ ซึ่งบริการเหล่านี้จะเป็นทางผ่านที่จะนำไปสู่การเข้าสู่ระบบของผู้บุกรุกจากภายนอกนั่นเอง นอกจากนั้นระบบปฏิบัติการคอมพิวเตอร์และส่วนการทำงานที่เกี่ยวข้องก็อาจจะมีจุดอ่อนจนเป็นผลทำให้สามารถเข้ามาทำลายระบบได้ ตัวอย่างของการทำงานที่ผิดพลาดได้แก่ การทำงานของบริการ **finger** ที่ผิดพลาดจนเป็นผลทำให้แฮกเกอร์เข้าสู่ระบบได้โดยอาศัยการรับอินพุตที่ผิดปกติเป็นต้น

ข้อผิดพลาดและจุดอ่อนของระบบยังรวมถึงการทำงานของโปรแกรมอื่นนอกเหนือจากโปรแกรมปกติที่อยู่ในระบบ ได้แก่ โปรแกรมอัตโนมัติที่แฮกเกอร์นำมาติดตั้งไว้ในระบบเพื่อทำงานบางอย่างหรือเพื่อขโมยข้อมูลบางอย่างของระบบ โปรแกรมเหล่านี้จะมีอันตรายมากหากได้มีการปลอมและแฝงตัวอยู่ในระบบจนผู้ดูแลระบบไม่สามารถจะตรวจได้พบ

วิธีการป้องกันและหลีกเลี่ยงไม่ให้เกิดเหตุการณ์เช่นนี้ ทำได้โดยการตรวจหาความผิดปกติใด ๆ ในระบบอยู่สม่ำเสมอ โดยหากเจอสิ่งที่ผิดปกติเกิดขึ้นควรจะตรวจสอบและจัดการกับปัญหาทันทีโดยไม่ปล่อยทิ้งไว้ นอกจากนั้นหากเป็นการใช้งานโปรแกรมหรือบริการที่มีข้อบกพร่องก็ควรปรับแก้โดยการนำซอฟต์แวร์รุ่นใหม่ ๆ มาติดตั้งแทนที่ให้เรียบร้อยถูกต้อง

ความผิดพลาดของการพิสูจน์ตัวจริง

กระบวนการติดต่อสื่อสารโดยส่วนใหญ่ในระบบเครือข่ายคอมพิวเตอร์จะอาศัยการพิสูจน์ตัวจริงเพื่อบ่งบอกถึงตัวตนที่แท้จริงของผู้จะติดต่อด้วยว่ามิใช่เป็นบุคคลอื่นหรือระบบอื่นที่ไม่ได้รับอนุญาตให้สื่อสารกัน เพราะฉะนั้นหากมีการพิสูจน์ตัวจริงเกิดขึ้นไม่สมบูรณ์หรือเกิดการผิดพลาดใด ๆ ขึ้น อาจจะทำให้แฮกเกอร์ซึ่งปลอมตัวมาสามารถเข้าสู่ระบบได้

บริการบางอย่างของระบบคอมพิวเตอร์มีความจำเป็นต้องอาศัยการพิสูจน์ตัวจริงที่เข้มงวดและในบางบริการก็ไม่เข้มงวดเพียงพอจนเป็นเหตุให้สามารถปลอมตัวแล้วเข้าสู่ระบบได้ ตัวอย่างเช่น เซิร์ฟเวอร์จะยอมให้บางโฮสต์เท่านั้นสามารถถ่ายโอนแฟ้มข้อมูลได้ หากแฮกเกอร์ปลอมเป็นโฮสต์ที่เซิร์ฟเวอร์เชื่อถือและเซิร์ฟเวอร์ก็ไม่สามารถจะพิสูจน์ได้ว่าโฮสต์นั้นปลอมและยอมให้มีการถ่ายโอนแฟ้มข้อมูลไปได้ ข้อมูลเหล่านั้นก็จะถูกลักลอบนำไปใช้งานได้

นอกจากการพิสูจน์ตัวจริงของโปรแกรมที่ให้บริการแก่ผู้ใช้งานแล้ว ในระดับของการส่งผ่านแพ็กเกตข้อมูลเองก็อาจมีการพิสูจน์ตัวจริงที่ไม่รัดกุมเพียงพอ เช่น โปรโตคอลไอพี (IP) ไม่มีกระบวนการที่จะรับประกันได้ว่าแพ็กเกตที่ส่งมานั้นถูกส่งมาจากไอพีแอดเดรสที่ระบุอยู่จริง ๆ หรือไม่ ซึ่งในบางครั้งอาจจะเป็นการสร้างแพ็กเกตโดยแฮกเกอร์แล้วระบุไอพีแอดเดรสต้นทางปลอมก็ได้

วิธีการแก้ปัญหาความผิดพลาดของการพิสูจน์ตัวจริงได้แก่ การสร้างกระบวนการพิสูจน์ตัวจริงที่รัดกุมยิ่งขึ้นทั้งในแง่ของโปรแกรมประยุกต์และโปรโตคอลที่ใช้งานในระดับล่าง นอกจากนั้นยังต้องกำหนดนโยบายการอนุญาตให้มีการติดต่อสื่อสารกันระหว่างโฮสต์ให้มีการรับประกันความถูกต้องของข้อมูลและมีการพิสูจน์ตัวจริงที่เหมาะสมด้วย

ความผิดพลาดของโปรโตคอล

การทำงานของโปรโตคอลอาจจะมีข้อผิดพลาดเกิดขึ้นได้ทั้งในแง่ของการทำงานพื้นฐานและการทำงานในออปชันพิเศษ โปรโตคอลบางชนิดถูกออกแบบมาให้ทำงานในสภาวะบางอย่างแต่ไม่เหมาะสมกับในอีกสภาวะก็อาจเป็นได้ ดังนั้นอาจมีความผิดพลาดเกิดขึ้นได้จากการทำงานของโปรโตคอล ซึ่งข้อผิดพลาดเหล่านี้อาจเป็นช่องทางทำให้เกิดการเจาะเข้าสู่ระบบได้

เป็นที่ทราบกันดีอยู่แล้วว่าในสารบบของการสื่อสารในเครือข่ายอินเทอร์เน็ตในปัจจุบันนั้นใช้โปรโตคอลทีซีพี/ไอพี (TCP/IP) เป็นชุดโปรโตคอลหลักในการกำหนดรูปแบบการส่งผ่านข้อมูลระหว่างกัน ถึงแม้ว่าทีซีพี/ไอพีจะถูกใช้งานมานานและดูเหมือนว่าจะมีประสิทธิภาพมาก แต่ก็มีการค้นพบจุดอ่อนและข้อผิดพลาดของการทำงานของโปรโตคอลหลาย ๆ ชนิด เช่น กระบวนการสถาปนาการเชื่อมต่อก่อนการส่งข้อมูลของโปรโตคอลทีซีพี เป็นต้น

ตัวอย่างที่เห็นได้ชัดเจนของการทำงานที่ผิดพลาดของโปรโตคอลได้แก่ การที่แฮกเกอร์สามารถเดาเลขลำดับ (Sequence number) ของแพ็กเกตได้ ซึ่งจะทำให้สามารถเข้ามาเชื่อมต่อกับระบบได้โดยที่ระบบจะไม่สามารถตรวจพบ วิธีการนี้มักจะถูกนำมาใช้โดยแฮกเกอร์ที่มีความรู้ด้านเทคนิคในเบื้องลึกทั้งในแง่ของระบบปฏิบัติการและระบบการสื่อสารของคอมพิวเตอร์

หากมีเหตุการณ์รูปแบบนี้เกิดขึ้น ผู้ดูแลระบบจำเป็นต้องพิจารณาดูว่ามีสาเหตุเกิดขึ้นจากส่วนใดหรือโปรโตคอลใด หากสามารถที่จะปรับแต่งเพื่อลดความเสียหายได้ก็ควรทำ แต่หากไม่สามารถทำได้ก็อาจจะต้องปิดการให้บริการหรืองดการทำงานของโปรโตคอลนั้นไปเพื่อความปลอดภัยของระบบ

การรั่วไหลของข้อมูล

ในบางกรณีข้อมูลเพียงเล็กน้อยก็มีประโยชน์ต่อการบุกรุกมาก ซึ่งหากแฮกเกอร์ได้รับข้อมูลส่วนนี้ไปก็จะทำให้สามารถเข้าสู่ระบบได้ สิ่งหนึ่งที่ต้องยอมรับคือผู้ดูแลระบบไม่สามารถที่จะปกป้องข้อมูลทั้งหมดไม่ให้รั่วไหลไปได้ เนื่องจากข้อมูลบางอย่างนั้นจำเป็นจะต้องแสดงหรือบ่งบอกให้ผู้ใช้งานปกติทราบ แต่หากผู้บุกรุกได้รับข้อมูลนี้ก็จะเป็นการสร้างความเป็นไปได้ที่จะเจาะระบบได้สะดวกยิ่งขึ้น

ตัวอย่างข้อมูลที่รั่วไหลได้แก่ เวอร์ชันของระบบปฏิบัติการ ข้อมูลที่รั่วไหลนี้ดูเหมือนจะไม่มีประโยชน์ต่อการบุกรุก แต่ในแง่ของผู้บุกรุกแล้วหากทราบมาก่อนว่าระบบปฏิบัติการเวอร์ชันใดมีจุดอ่อนอะไรและสามารถเจาะเข้าได้ทางใดแล้ว หากเพียงแค่ทราบว่าเซิร์ฟเวอร์ใดบ้างที่ใช้ระบบปฏิบัติการนั้นอยู่ก็จะสามารถทำลายระบบได้ บริการ **login** เป็นตัวอย่างหนึ่งที่เห็นได้ชัดเจนว่าได้แสดงข้อมูลเหล่านี้ไว้อย่างครบถ้วน ดังรูปที่ 3

```
[user@host user]$ telnet host.domain.com
Trying 0.0.0.0...
Connected to 0 (0.0.0.0).
Escape character is '^]'.

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0 on an i586
login:
```

รูปที่ 3 ข้อมูลที่ได้จากบริการ login

การปฏิเสธการให้บริการ

การปฏิเสธการให้บริการหรือที่เรียกว่าดอส (DoS : Denial-of-Service) เป็นรูปแบบการบุกรุกที่ทำให้ระบบไม่สามารถให้บริการบางอย่างได้ตามปกติ เช่น เมื่อเกิดเหตุการณ์บุกรุกระบบคอมพิวเตอร์แล้ว จะส่งผลให้ระบบไม่สามารถให้บริการได้การปฏิเสธการให้บริการจะเกิดขึ้นเนื่องมาจากสาเหตุหลาย ๆ ประการ เช่น ข้อจำกัดของการให้บริการ หรือข้อจำกัดของทรัพยากรของระบบ เป็นต้น

ตัวอย่างของการปฏิเสธการให้บริการที่เห็นได้ชัดเจน เช่น การโจมตีด้วยแพ็กเกต SYN จนเป็นผลทำให้เว็บเซิร์ฟเวอร์ไม่สามารถให้บริการได้ตามปกติ การโจมตีแบบนี้อาศัยจุดอ่อนของการออกแบบการเชื่อมต่อระหว่างโฮสต์ที่ใช้โปรโตคอลทีซีพีในการสถาปนาการเชื่อมต่อ ผู้บุกรุกจะสร้างแพ็กเกตขอสถาปนาการเชื่อมต่อไปยังเซิร์ฟเวอร์จำนวนมากและไม่ยอมให้มีการสถาปนาการเชื่อมต่อให้สำเร็จ ทำให้เซิร์ฟเวอร์ต้องจองทรัพยากรไว้จำนวนมากจนไม่สามารถรองรับการเชื่อมต่อใหม่ ๆ ได้อีก ซึ่งเป็นที่มาของการปฏิเสธการติดต่อสื่อสารต่อไปนั่นเอง

วิธีการแก้ไขอาจทำได้โดยการปรับค่าของกระบวนการทำงานของส่วนให้บริการมิให้ปฏิเสธการให้บริการหรือปฏิเสธการให้บริการเร็วเกินไป นอกจากนั้นอาจให้อุปกรณ์เครือข่ายอื่น ๆ เช่น เราเตอร์ช่วยในการกรองแพ็กเกตข้อมูลที่ผิดปกติมิให้เข้ามาทำลายระบบได้ด้วย

สรุป

จากรูปแบบการบุกรุกทั้ง 7 แบบดังกล่าวจะเห็นได้ชัดเจนว่าแต่ละแบบจะมีลักษณะพิเศษที่แตกต่างกันไป และแต่ละชนิดก็ก่อให้เกิดความเสียหายที่ไม่เหมือนกันด้วย เหตุการณ์ที่ผิดปกติในบางครั้งไม่สามารถจัดให้อยู่ในกลุ่มใดใน 7 กลุ่มนี้ได้โดยเฉพาะเพียงกลุ่มเดียว แต่ในบางครั้งจะเป็นการผสมผสานระหว่างกลุ่มก็อาจเป็นได้ สิ่งสำคัญที่สุดก็คือ ผู้ที่ตรวจพบจะต้องสามารถแยกแยะเหตุการณ์ผิดปกติเหล่านั้นและอธิบายถึงลักษณะของการบุกรุกได้อย่างชัดเจนและมีหลักเกณฑ์ที่ถูกต้องเพื่อจะนำไปสู่การป้องกันในอนาคต